

\*\*\*PUBLIC VERSION\*\*\*

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

UNITED STATES OF AMERICA,

Plaintiff,

v.

ZACKARY ELLIS SANDERS,

Defendant.

Case No. 1:20-cr-00143  
The Honorable Judge Ellis  
Hearing: Sept. 11, 2020

**MEMORANDUM IN SUPPORT OF MR. ZACKARY ELLIS SANDERS'S MOTION TO  
SUPPRESS BASED ON FALSE AND MISLEADING MATERIAL INFORMATION IN  
AFFIDAVIT PARAGRAPH 25 (Motion to Suppress No. 4)**

Jonathan Jeffress (#42884)  
Emily Voshell (#92997)  
Jade Chong-Smith (admitted *pro hac vice*)  
KaiserDillon PLLC  
1099 14<sup>th</sup> Street. NW  
8<sup>th</sup> Floor West  
Washington, D.C. 20005  
Telephone: (202) 683-6150  
Facsimile: (202) 280-1034

*Counsel for Defendant Zackary Ellis Sanders*

**TABLE OF CONTENTS**

EXHIBITS INDEX .....	iii
INTRODUCTION .....	1
PROCEDURAL HISTORY .....	4
A. The Search Warrant. ....	4
B. Mr. Sanders’s Initial Appearance, Detention Hearing, Indictment, and Arraignment. ....	5
C. Mr. Sanders’s Motion to Compel Discovery. ....	5
D. The Court’s Memorandum Opinion.....	7
BACKGROUND .....	8
A. [REDACTED] .....	8
THE LAW OF FRANKS v. DELAWARE .....	11
ARGUMENT .....	12
I. THE FBI KNOWINGLY AND RECKLESSLY MISLED THE MAGISTRATE IN [REDACTED] .....	12
1. There is no process [REDACTED] [REDACTED] .....	13
2. The Special Agent was not aware of any method that could [REDACTED] [REDACTED] .....	15
3. The Special Agent knew [REDACTED] [REDACTED] .....	15
4. [REDACTED] .....	16
II. MR. SANDERS HAS BEEN DENIED FURTHER DISCOVERY REQUIRED TO SHOW CONCLUSIVELY [REDACTED] [REDACTED] .....	17
III. ALL FRUITS OF THE ILLEGAL SEARCH MUST BE SUPPRESSED.....	20
CONCLUSION.....	20

**EXHIBITS INDEX**

Exhibit #	Title
1	██████████
2	██████████
3	██████████
4	Declaration of Dr. Matthew Miller
5	Third Declaration of Dr. Matthew Miller
6	Fourth Declaration of Dr. Matthew Miller
7	Declaration of Mathew Ryder QC
8	Second Declaration of Matthew Ryder QC
9	Declaration of Dr. Richard Clayton
10	Matish Affidavit
11	Comparison Report of <i>Matish</i> Affidavit and <i>Sanders</i> Affidavit
12	██

Zackary Ellis Sanders, by and through undersigned counsel, and pursuant to Federal Rule of Criminal Procedure 41 and the Fourth Amendment, respectfully moves this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case because the Special Agent recklessly misled the Magistrate about how the Internet user was identified, which goes directly to the tipster's (the Foreign Law Enforcement Agency's) credibility, as well as the Special Agent's credibility, and was necessary to the Magistrate finding probable cause to issue the warrant.

### **INTRODUCTION**

The Federal Bureau of Investigation ("FBI") was investigating a website called [REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Ex. 1 (Intel Log). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FBI Special Agent [REDACTED] (“the Special Agent”) should have known—from

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]. Contrary to the Special Agent’s [REDACTED]

[REDACTED] the FBI either knew or should have known [REDACTED]  
[REDACTED]  
[REDACTED] without informing the Magistrate of its false and misleading nature violated Mr. Sanders’s rights under the Fourth Amendment and requires a hearing under *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978).

While academics have discussed other methods that do not interfere with an Internet user’s computer as being theoretically possible, [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] Ex. 5 (Third Declaration of Dr. Matthew Miller); Ex. 9 (Declaration of Dr. Richard Clayton).

If the Special Agent was the expert he presented himself as, then he knew that to be the case. *See*

---

<sup>1</sup> The Affidavit refers to [REDACTED].” The Government has disclosed no communications from the FBI to the [REDACTED]—the documents that would most clearly convey the FBI’s true understanding of how the [REDACTED] identified the Internet user in this case and how that understanding conflicts with the Affidavit. This failure was the subject of the Court’s August 21, 2020 Memorandum Opinion (ECF No. 73). Given the additional information before the Court, Mr. Sanders has respectfully asked to renew his Motion to Compel, or, in the alternative, for the Court to reconsider its erroneous denial of his Motion to Compel.

Ex. 5 (Third Declaration of Dr. Matthew Miller) at 2; Ex. 9 (Declaration of Dr. Richard Clayton) at 8 (explaining why “the academic material cited by [Special Agent] Ford on August 10<sup>th</sup> is entirely irrelevant and entirely beyond the state of the art. No-one who has any familiarity with practical attacks on anonymity systems should believe that the global passive adversary exists”).

[REDACTED]  
[REDACTED] the Special Agent should have known [REDACTED]  
[REDACTED]  
[REDACTED]. *Id.* at 8-9. And therefore, that [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] The FBI cannot procure illegally obtained evidence [REDACTED] and then mislead the Magistrate about how that evidence was obtained. Gov’t Opp’n (ECF No. 41) at 16.

Based on the scant discovery the Government has provided to date, the Government’s own statements, and the declarations submitted by four defense experts,<sup>2</sup> Mr. Sanders has made “a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit.” *Franks*, 438 U.S. at 155–56. The Affidavit misled the Magistrate into drawing the incorrect inference the Special Agent knew or should have known was incorrect: that the process used to identify the Internet user’s IP address did not involve interfering with a computer in the United States and that

---

<sup>2</sup> The declarants are Dr. Matthew Miller, Associate Professor Computer Science and Information Technology at the University of Nebraska at Kearney; Matthew Ryder QC, U.K. barrister and part-time judge in higher criminal courts; Seth Schoen, computer technologist and privacy specialist who worked as a Senior Staff Technologist at the Electronic Frontier Foundation for the past 19 years; and Dr. Richard Clayton, Director of the Cambridge Cybercrime Centre at the University of Cambridge.

it had therefore not violated the Fourth Amendment. Had the Magistrate known that [REDACTED] [REDACTED] the Magistrate could not have found probable cause because that would have directly undermined both the [REDACTED]'s and the Special Agent's credibility. Particularly when the false statements are excised from the Affidavit and Paragraph 25 is corrected to explain the NCA's use of Equipment Interference against many people's computers, no neutral Magistrate would have issued the warrant. As a result, Mr. Sanders requests, and is respectfully entitled to, a *Franks* hearing. *Id.* ("[I]f the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request").

Because the warrant was based on materially false statements and omissions, the good faith exception under *United States v. Leon*, 468 U.S. 897, 932 (1984) does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home, the interrogation of Mr. Sanders and his parents, and the forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

## **PROCEDURAL HISTORY**

### **A. The Search Warrant.**

[REDACTED] That same day, the Magistrate issued a warrant for the FBI to search the Sanders's family home. The circumstances of the execution of the search warrant are set forth in the Memorandum in Support of Mr. Sanders's Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1) at 2-3.

## **B. Mr. Sanders's Initial Appearance, Detention Hearing, Indictment, and Arraignment.**

On March 20, 2020, over five weeks later, Mr. Sanders was arrested and made his initial appearance. On June 24, 2020, based on the evidence derived from the illegal search of the Sanders's family home, Mr. Sanders was indicted on five counts of production of child pornography in violation of 18 U.S.C. § 2251 (a) and § 2251(e), six counts of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and § 2252(b)(1), and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and § 2252(b)(2). Mr. Sanders faces a mandatory minimum of fifteen years in prison for each count of production of child pornography.<sup>3</sup>

At arraignment on July 10, 2020, Mr. Sanders appeared before this Court and his counsel explained that he had a meritorious motion to suppress and for a *Franks* hearing, but that the Government was refusing to provide additional discovery in its possession, custody, or control relevant to that motion to suppress. The Court set a schedule for Mr. Sanders to submit a motion to compel and, once the Court had resolved that motion, a motion to suppress.<sup>4</sup>

### C. Mr. Sanders's Motion to Compel Discovery.

The Government produced no communications from the FBI to the ██████ regarding Mr. Sanders's case, while also not denying, however, that such communications do exist.<sup>5</sup>

On July 13, 2020, and based on the Government's refusal to produce further discovery, Mr. Sanders moved to compel discrete categories of discovery. Mot. to Compel (ECF No. 37). The

3 [REDACTED]

<sup>4</sup> On August 20, 2020, the Court extended the pretrial motions deadline to August 27, 2020.

5. [REDACTED]



requested discovery would further establish that the Special Agent knew (or should have known)

██████████ *Id.* Mr. Sanders noted that he had submitted detailed discovery requests to the Government regarding the Government's contemporaneous understanding of ██████████

The Government, notwithstanding its obligations under Rule 16(a) and *Brady v. Maryland*, 373 U.S. 83 (1963), had refused to provide Mr. Sanders with meaningful discovery regarding the [REDACTED] the Internet user's IP address, among other issues. This discovery was and is critical to Mr. Sanders's motion to suppress. *Id.* at 2.

On July 27, 2020, the Government filed an Opposition to Mr. Sanders’s Motion to Compel Discovery. Gov’t Opp’n (ECF. No. 41). On August 10, 2020, Mr. Sanders and Government filed supplemental briefs. *See* Defense Brief (ECF No. 51); Gov’t Brief (ECF No. 53). In its supplemental brief, the Government declined to explain to the Court what the Special Agent actually understood about how [REDACTED] the Internet user’s IP address at the time he submitted the Affidavit—and whether it contradicts what the defense had alleged—*despite submitting a Declaration from the Special Agent himself*. Ex. 12 (Aug. 10 Declaration of Special Agent Ford). Instead, the Special Agent discussed purely hypothetical methods that do not work in practice and that he was apparently not aware of at the time he submitted the Affidavit. *See, e.g.* Third Declaration of Dr. Matthew Miller (Ex. 5) at 2; Declaration of Richard Clayton (Ex. 9) at 8.

On August 12, 2020, Mr. Sanders filed a response to the Government’s Brief. Response to Gov’t Brief (ECF No. 64).

**D. The Court's Memorandum Opinion.**

On August 21, 2020 the Court issued an Order (ECF No. 74) denying Mr. Sanders's Motion to Compel Discovery. In a Memorandum Opinion (ECF No. 73) accompanying the Court's Order, the Court rejected Mr. Sanders's central argument that the Government was in possession of further communications and documents relevant to Mr. Sanders's motion to suppress that it was refusing to produce. *Id.* at 9.

On the issue of [REDACTED], the Court's Memorandum Opinion reflects, respectfully, a factual error: the Special Agent's Declaration does not describe "alternative, publicly known methods of de-anonymizing Tor users without interfering with a Tor user's computer" that *actually work in practice* or that could have successfully identified an Internet user based only on a single visit to a website. Memorandum Opinion (ECF No. 73) at 12. Dr. Matthew Miller and Dr. Richard Clayton explain why that is incorrect. Ex. 5 (Third Declaration of Dr. Matthew Miller) at 2 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]; Ex. 9 (Declaration of Dr. Richard Clayton) at 8 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**BACKGROUND**

A. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

6.

6

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

In the Eastern District of Virginia, FBI Special Agent Douglas Macfarlane swore two Affidavits for search warrants to deploy an NIT on a target website to seize the true IP addresses of people who logged into the website by entering a username and password. He stated:

Due to the unique nature of the Tor network and the method by which the network protects that anonymity of its users by routing communications through multiple other computers or ‘nodes,’ . . . *other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried.* . . . Under the NIT authorized by this warrant, the TARGET WEBSITE . . . would augment that content [that websites send to visitors in the normal course of operation] with additional computer instructions . . . designed to cause the user’s ‘activating’ computer to transmit certain information to a computer controlled by or known to the government. . . . *to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information, . . . such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation.*

*United States v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016) (ECF No. 18-2 at 24-25, 29) (emphasis added);<sup>7</sup> *see also United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016) (ECF No. 23-2 at 27-28, 32) (exact same) (emphasis added).

FBI agents have testified to the same in court. As FBI Special Agent Steven Smith previously testified:

In the case of a Tor hidden service, once we seize that website, we don’t know the true IP address of the users, so we’re not able to trace back who those users are. We only would be able to see, at most, the last node in the connection. That would be the IP address available to us. And we would not be able to trace back to the originating IP address. . . . *We have to have a method in which we can proactively, once we seize the website, attempt to ascertain the user’s true IP address and we typically do this through network investigative technique . . . to cause the user’s computer to communicate with an FBI-controlled computer outside the Tor network.*

---

<sup>7</sup> Special Agent Douglas McFarlane’s affidavit in *U.S. v. Matish* contains a significant amount of language that is extremely similar and in some cases identical [REDACTED]. Compare Ex. 10 (*Matish* Affidavit) with Ex. 3 (Affidavit); *see also* Ex. 11 [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

*United States v. Cottom*, No. 8:13CR108, 2013 WL 6567553 (D. Neb. Dec. 12, 2013) (ECF No. 257 at 21) (emphasis added).

FBI Special Agent Daniel Alfin, who was the case agent for the national Playpen investigation in multiple jurisdictions, previously testified that it was “correct” that when Internet users “access[ed] the site using the Tor Browser . . . *you’re required to send some kind of additional exploit to get code to execute on their computer . . . because of a feature in Tor . . . to prevent someone from learning the Tor Browser user’s true IP address.*” *United States v. Wheeler*, No. 1:15-CR-390 (N.D. Ga. Aug. 21, 2017) (emphasis added). He later testified:

So the Playpen website was a child pornography website that existed within the Tor network running as a Tor hidden service. . . *because it’s running as a Tor hidden service*, even though we now have control of the website, *we still don’t know who the users are. People can still access the website but we can’t see their real IP address. So that’s what the NIT does.* . . [W]hen you access the internet through Tor, your real IP address is invisible to the destination. *So what the NIT does is it forces the computer to communicate outside of the Tor network over the regular internet. So when that happens, we can see the defendant’s real IP address.*

*United States v. Stamper*, Case No. 1:15cr109 (S.D. Ohio Mar. 9, 2018) (ECF No. 94 at 69, 75-76) (emphasis added).

### **THE LAW OF FRANKS V. DELAWARE**

In *Franks v. Delaware*, the Supreme Court set forth a two-step test for defendants to challenge the veracity of an affidavit in support of a search warrant. 438 U.S. 154, 155-56 (1978); accord *United States v. Clenney*, 631 F.3d 658, 663 (4th Cir. 2011).

First, Mr. Sanders must “make[] a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s request.” *Franks*,

438 U.S. at 155–56; *see also United States v. Leonard*, No. 17-cr-135, 2017 WL 4478330 at \*5 (E.D. Va. October 6, 2017) (similar). “This showing must be more than conclusory and should include affidavits or other evidence to overcome the presumption of the warrant’s validity.” *Clenney*, 631 F.3d at 663 (quotation marks and internal punctuation omitted).

Second, at the *Franks* hearing, Mr. Sanders must establish “the allegation of perjury or reckless disregard . . . by a preponderance of the evidence.” *Franks*, 438 U.S. at 156. Furthermore, “with the affidavit’s false material set to one side, the affidavit’s remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.” *Id.* at 156. “A warrant that violates *Franks* is not subject to the good-faith exception to the exclusionary rule.” *Colkley*, 899 F.2d 297 at 300.<sup>8</sup>

## **ARGUMENT**

### **I. THE FBI KNOWINGLY AND RECKLESSLY MISLED THE MAGISTRATE IN PARAGRAPH 25 OF THE AFFIDAVIT.**

The FBI, based on the information that it received [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>8</sup> Mr. Sanders hereby further incorporates by reference the section on the Law of *Franks v. Delaware* of the Memorandum in Support of his Motion to Suppress Based on False and Misleading Information [REDACTED] (Motion to Suppress No. 2).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**A. There is no process for** [REDACTED]  
[REDACTED]

What FBI Agents have previously stated under oath is substantively [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED] Ex. 5 (Third Declaration of Dr. Matthew Miller) at 1.

[REDACTED]

---

<sup>9</sup> Dr. Miller has previously been qualified as an expert in numerous previous cases that involved child pornography investigations on the Tor network, and the defense is not aware of any instance where the Government objected to Dr. Miller's expertise.

[REDACTED]

**B. The Special Agent was not aware of any method that could s** [REDACTED]

[REDACTED]

**C. The Special Agent knew** [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**D.** [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

E. [REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

II. **MR. SANDERS HAS BEEN DENIED FURTHER DISCOVERY REQUIRED TO SHOW CONCLUSIVELY THAT THE NCA VIOLATED U.S. LAW AND THAT THE FBI REQUIRED AN EARLIER WARRANT BEFORE ITS INVESTIGATORY PARTNER USED EQUIPMENT INTERFERENCE IN THE U.S.**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The Court denied Mr. Sanders's motion to compel such documents, which would have demonstrated that [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] *Id.* at

9.

Thus, had this Court granted Mr. Sanders's motion to compel, Mr. Sanders would have been able to show two things conclusively. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Given intelligence-sharing agreements between [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] *it is precisely why the Framers enacted the Fourth Amendment in the first place. Riley v. California*, 573 U.S. 373, 403 (2014) (the Fourth Amendment was meant to protect against “the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity”).

The Fourth Amendment’s prohibition against unreasonable searches and seizures required the Government [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Assuming, *arguendo*, that Mr. Sanders went on Tor and his personal electronic devices would have contained traces of his browsing activity on the Tor Browser (which they would not have), Mr. Sanders had a reasonable expectation of privacy in his IP address and browsing activity on the Tor network. While something “a person knowingly exposes to the

---

<sup>10</sup> Intelligence and Security Committee of Parliament, Parliament of the United Kingdom, *Privacy and Security: A modern and transparent legal framework* 90-91 (March 2015) (describing how the U.K. shares information with overseas partners, including with members of the Five-Eyes network, which includes the U.S.), available from <https://isc.independent.gov.uk/committee-reports/special-reports>.

public” is not constitutionally protected, something a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” *Katz v. United States*, 389 U.S. 347, 351 (1967). People have a reasonable expectation of privacy when using the Tor network because “only the IP address of the last relay computer . . . as opposed to the Tor user’s actual IP address, appears on that website’s IP address log,” and furthermore, “the content of a Tor user’s communications are encrypted while the communication passes through the Tor network.” Ex. 3 (Affidavit) at ¶ 11; *see also* Ex. 4 (Declaration of Dr. Matthew Miller); Ex. 6 (Fourth Declaration of Dr. Matthew Miller); Ex. 9 (Declaration of Richard Clayton). Even though the Tor Project has a publicly available webpage that cautions “that the use of the Tor network does not render a user’s communication totally anonymous,” Ex. 3 (Affidavit) at ¶ 12, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### **III. ALL FRUITS OF THE ILLEGAL SEARCH MUST BE SUPPRESSED.**

All tainted fruits, including tangible evidence, electronic evidence, and statements Mr. Sanders made to law enforcement, should be suppressed. The facts and law in support of why all illegal fruits must be suppressed is set forth in the Memorandum in Support of Mr. Sanders’s Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1) at 14-15.

### **CONCLUSION**

Because the warrant issued in this case was on materially false statements and omissions, the good faith exception under *United States v. Leon*, 468 U.S. 897, 932 (1984) does not apply.

As a result, all evidence derived from the illegal search of the Sanders's family home, the illegal interrogation of Mr. Sanders and his parents, and the illegal forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

Respectfully submitted,

/s/ Jonathan Jeffress

Jonathan Jeffress (#42884)  
Emily Voshell (#92997)  
Jade Chong-Smith (admitted *pro hac vice*)  
KaiserDillon PLLC  
1099 Fourteenth St., N.W.; 8th Floor—West  
Washington, D.C. 20005  
Telephone: (202) 683-6150  
Facsimile: (202) 280-1034  
Email: jjeffress@kaiserdillon.com  
Email: evoshell@kaiserdillon.com  
Email: jchong-smith@kaiserdillon.com

*Counsel for Defendant Zackary Ellis Sanders*